Cost Estimation of Cybersecurity in Acquisition Programs: IMDE Primer

Joint IT and Software Cost Forum 2022

Alex Hoover

Ekaterina Brancato

Grace Shin

Outline of the Presentation

What is IMDE?	And why you should care
Problem statement	Knowledge gap between operational and technical risks
IMDE methodology	Identify risks early
Customizing WBS	Show WBS and dictionary

What is IMDE?

- A platform and supporting policy, process and governance, that facilitates federation of operational data, to enable enhanced situational awareness, mission planning, and coordination across DHS and the Homeland Security Enterprise.
- Three-pronged approach to DHS enterprise data federation
    1. Data Federation Engine with granular access controls
    2. Coordinated Enterprise Data Stewardship (non-materiel)
    3. Shared Enterprise Data Services

Problem Statement

Many software projects experience budget and schedule overruns due to poorly defined requirements at the onset

Enterprise-level projects have feature complexity, require rigorous requirements and are especially prone to catastrophic failure

Most cybersecurity failures are detected after compromise, without the opportunity to mitigate the problems over time

Most focus in programs is to cybersecurity technical controls; the policy and operational controls related to feature complexity are equally as important

Our Methodology

Approach policy, operational, and technical controls holistically

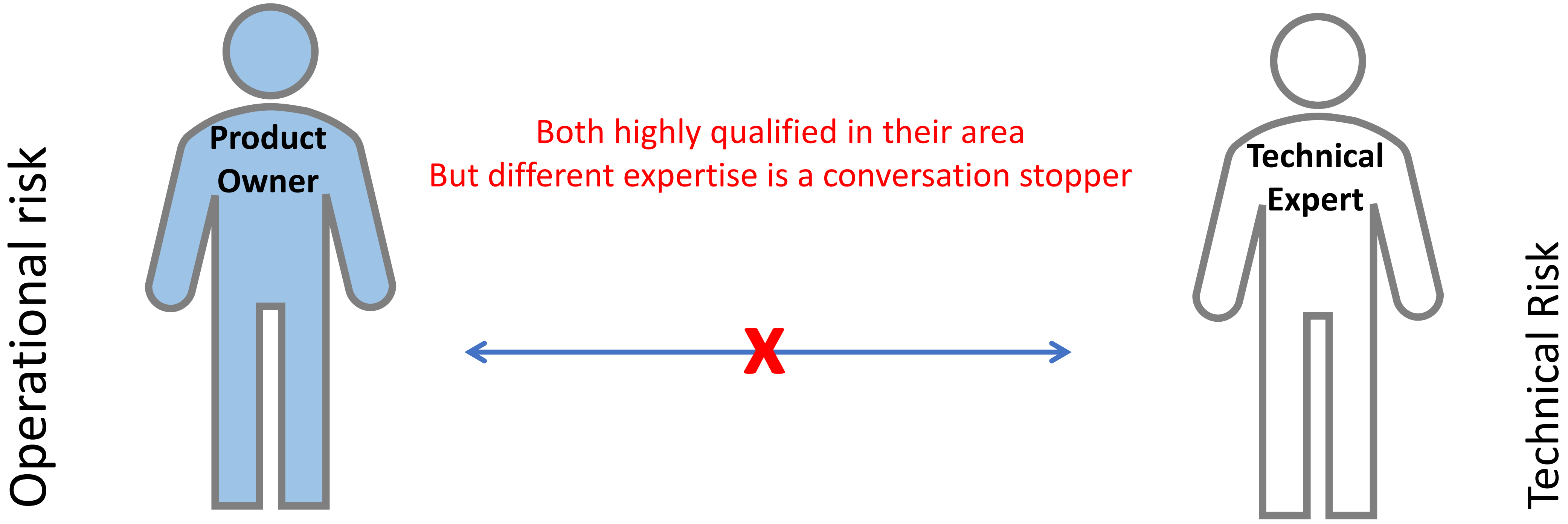
Identify specific operational risk cyber activities in IMS; Align to WBS

Choose balanced federal and contractor expertise

Limit resources allocated to lower benefit measures

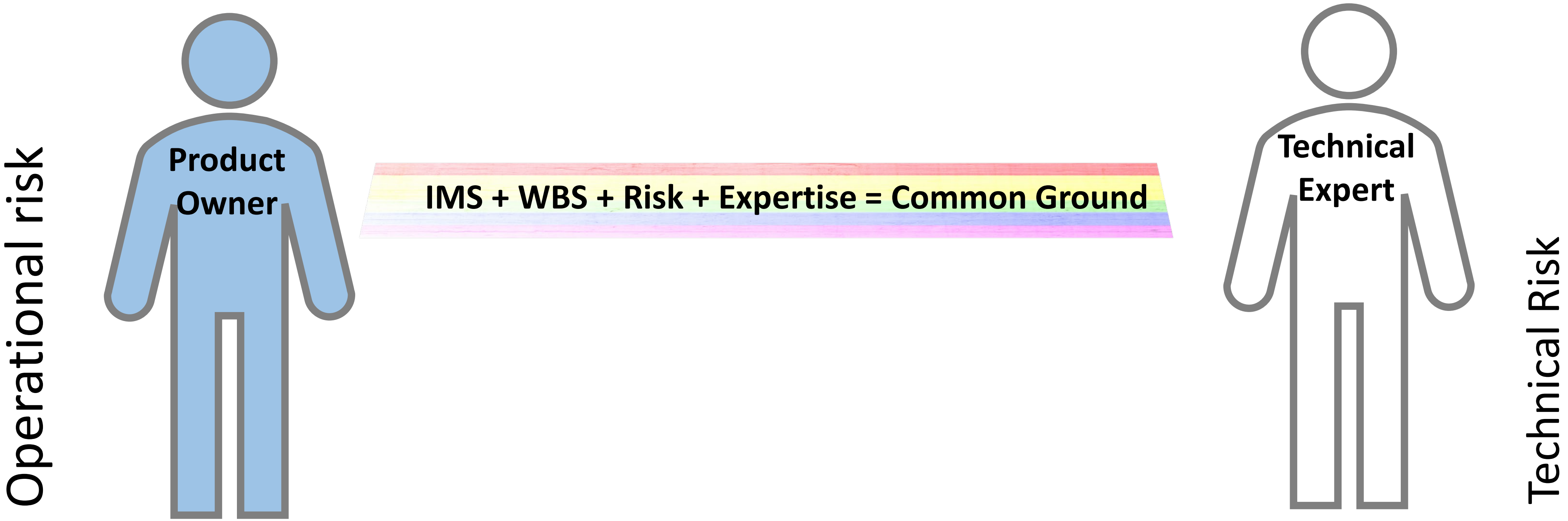
Knowledge Exchange Gap

- As projects become more complex and require more specialized expertise and division of labor, the right way to collaborate is turning point of success vs failure


Operational risk
Product Owner
Both highly qualified in their area
But different expertise is a conversation stopper
X
Technical Expert
Technical Risk

Bridging the Gap

- Structuring large amount of info helps its comprehension and consistency (risks drivers for security), that is the general purpose of product and action-based WBS



Operational risk

Product Owner

IMS + WBS + Risk + Expertise = Common Ground

Technical Expert

Technical Risk

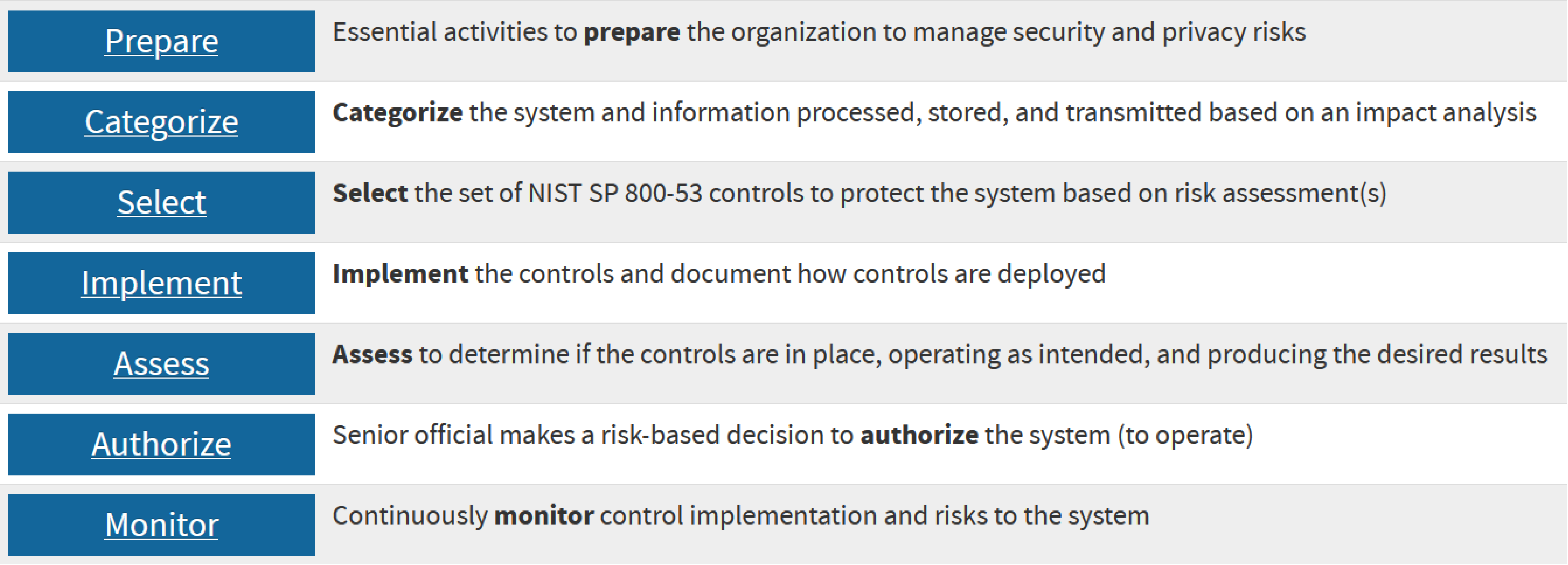
Common Practice

- There are several risk mitigating frameworks and standards
  - For example, the ISO 27000 series, ISF SOGP, NIST 800 series, SOX, and Risk IT
  - Concentrating on security concerns, these do not make a specific point of bridging the gap between technical approach and operational risk at an early stage
- Risk Breakdown Structure (RBS)
  - Hierarchical structure of potential risk sources
- Risk cube
  - Subjective, does not address lowest level elements

Best Practice

- **Common Practice + addresses operational aspects**
- IMDE WBS expansion prior ADE-2A
  - DHS Standard IT LCC WBS
  - Added additional elements that refer to risks
  - Different elements for:
    - Acquisition and planning stage
    - Program Mgmt, Systems Engineering, BPR
- Choose operational controls early on
- Identify cost contributors, avoid wasting scarce resources and cost overruns

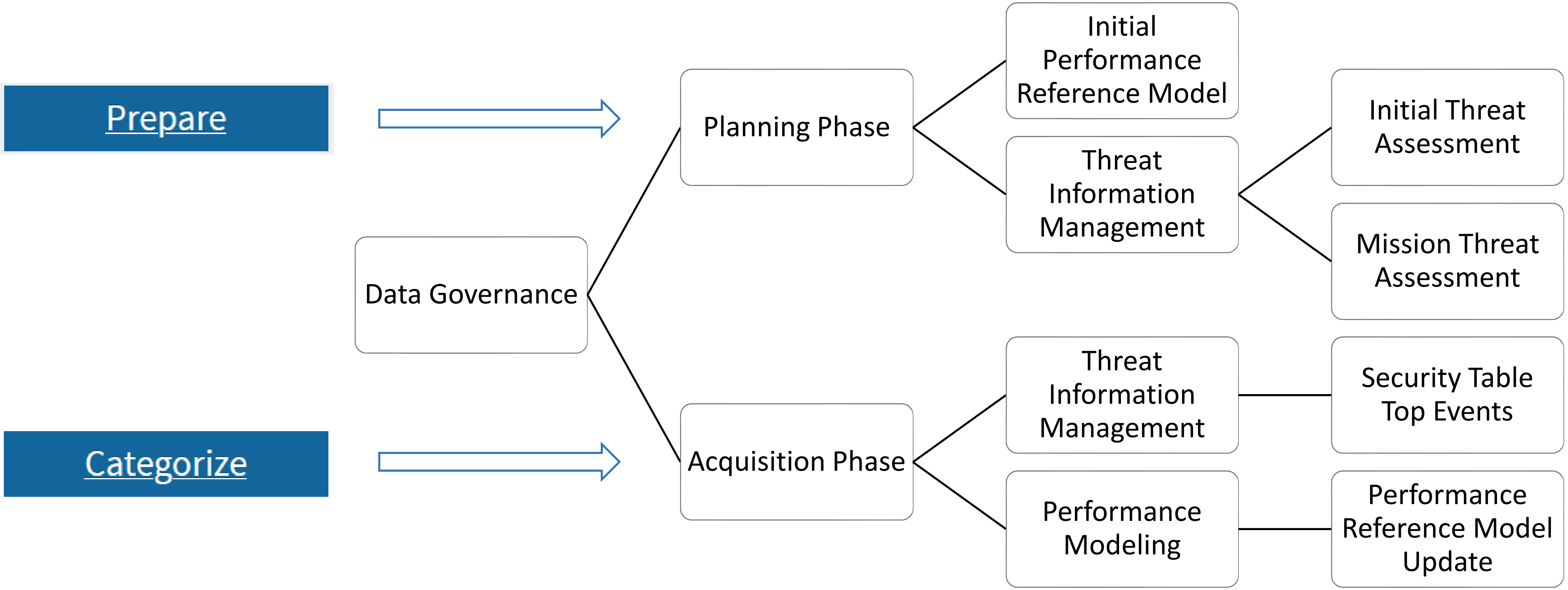
Risk Management Framework (RMF)



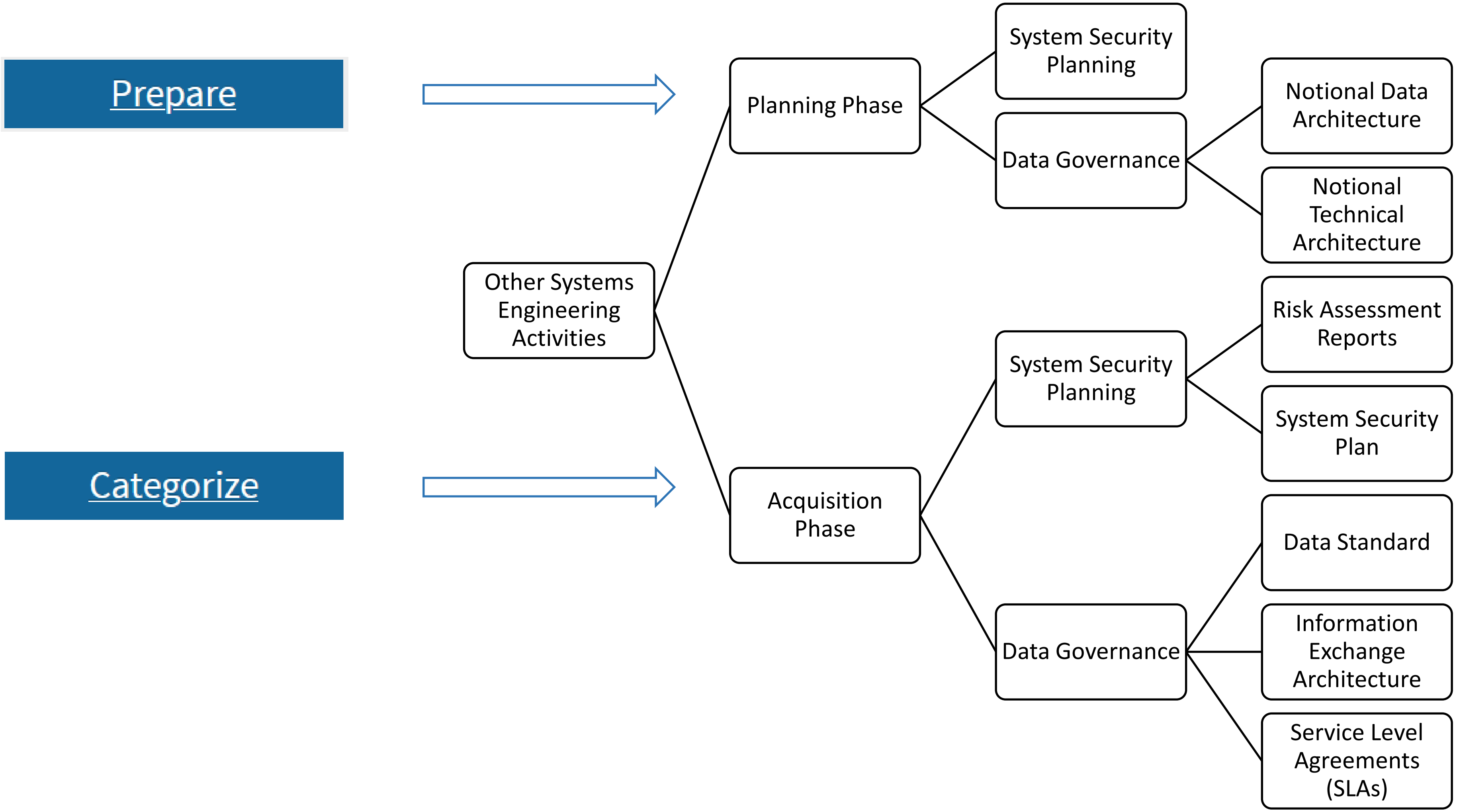
Prepare	Essential activities to **prepare** the organization to manage security and privacy risks
Categorize	**Categorize** the system and information processed, stored, and transmitted based on an impact analysis
Select	**Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
Implement	**Implement** the controls and document how controls are deployed
Assess	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to **authorize** the system (to operate)
Monitor	Continuously **monitor** control implementation and risks to the system

RMF and IMDE: Data Governance

IMDE early-stage risk identifying activities: added WBS elements under Prepare and Categorize


Prepare
Categorize
Data Governance
Planning Phase
Acquisition Phase
Initial Performance Reference Model
Threat Information Management
Initial Threat Assessment
Mission Threat Assessment
Threat Information Management
Performance Modeling
Security Table Top Events
Performance Reference Model Update

RMF and IMDE: Other Systems Engineering Activities

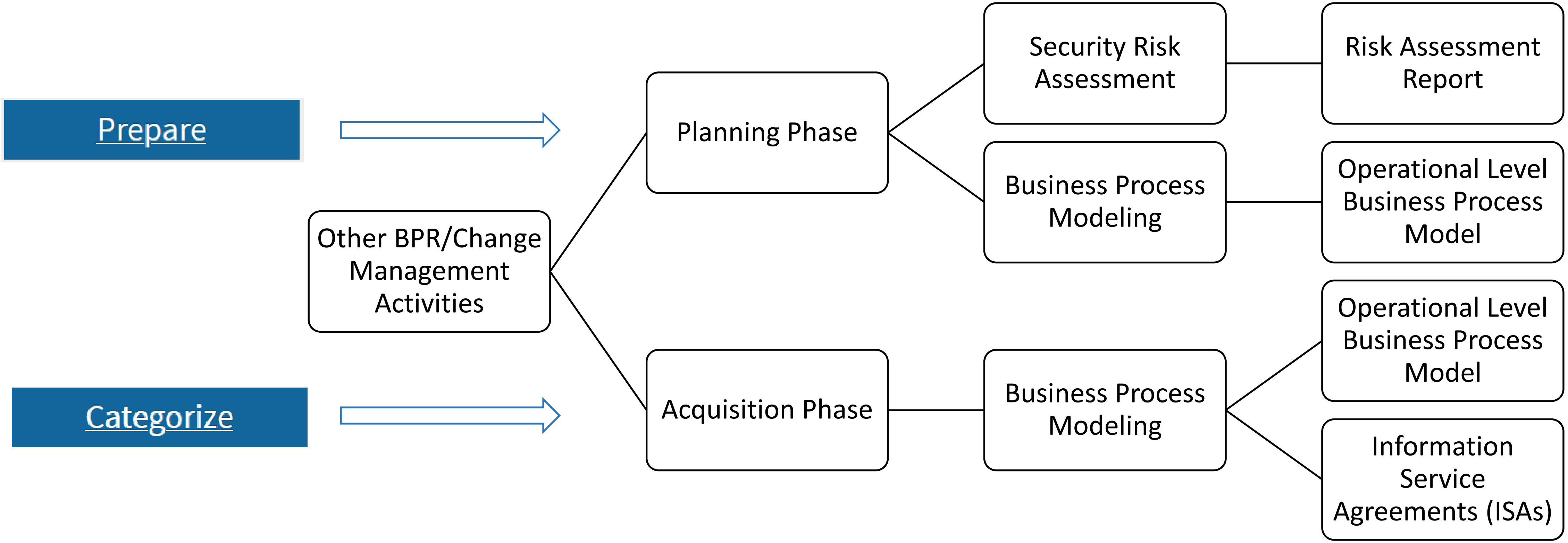


Prepare

Categorize

- Other Systems Engineering Activities
  - Planning Phase
    - System Security Planning
    - Data Governance
      - Notional Data Architecture
      - Notional Technical Architecture
  - Acquisition Phase
    - System Security Planning
      - Risk Assessment Reports
      - System Security Plan
    - Data Governance
      - Data Standard
      - Information Exchange Architecture
      - Service Level Agreements (SLAs)

RMF and IMDE: Other BPR/Change Management Activities



Prepare

Categorize

Other BPR/Change Management Activities

Planning Phase

Security Risk Assessment

Risk Assessment Report

Business Process Modeling

Operational Level Business Process Model

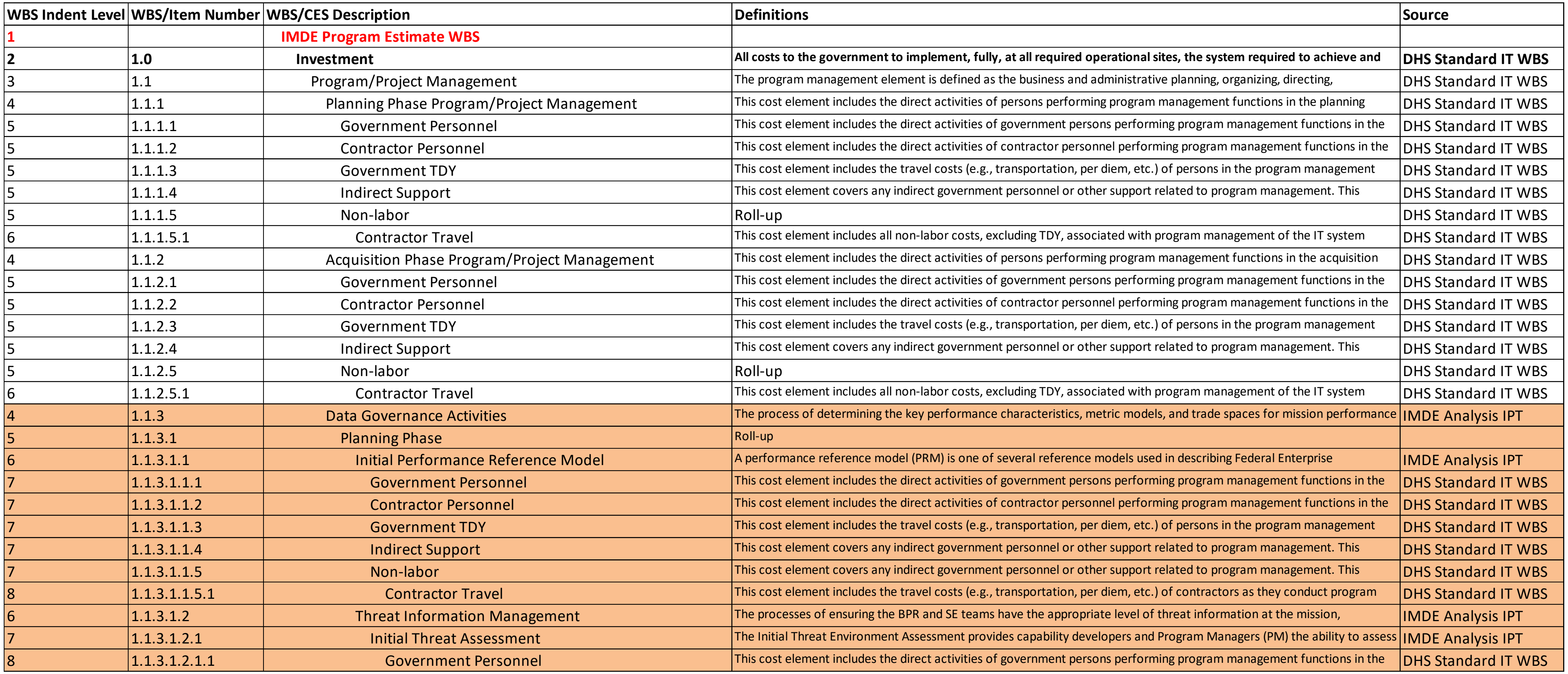
Acquisition Phase

Business Process Modeling

Operational Level Business Process Model

Information Service Agreements (ISAs)

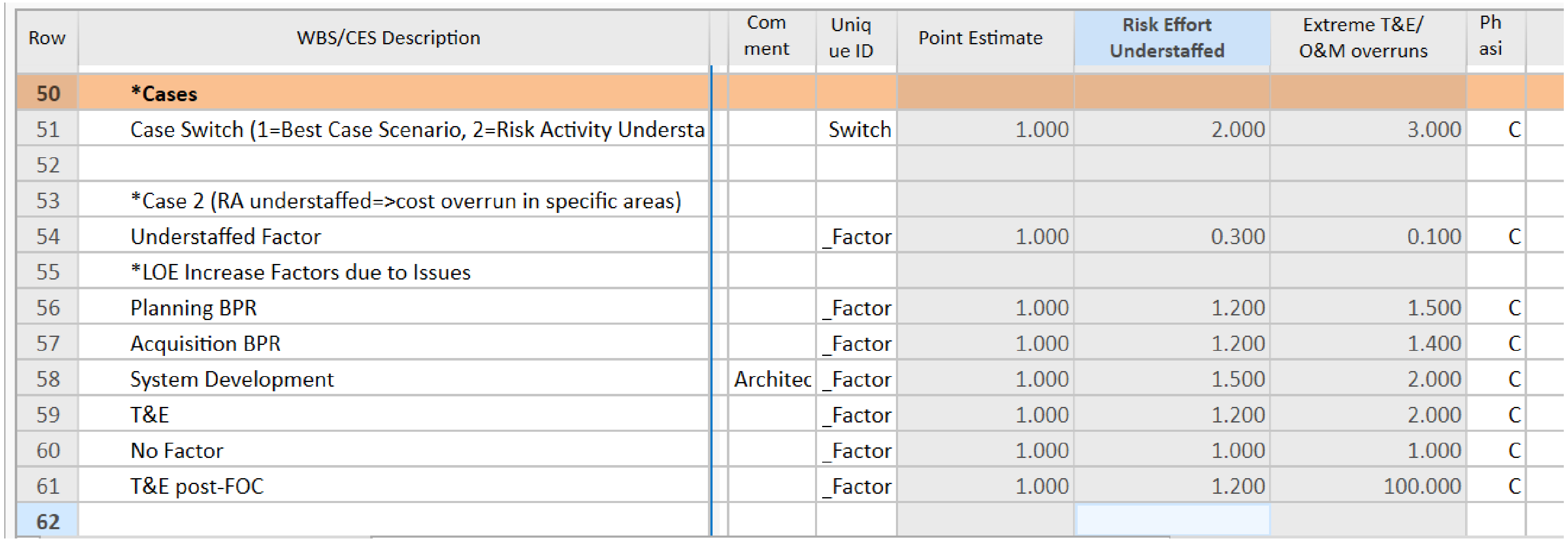
Embed IMDE WBS



WBS Indent Level	WBS/Item Number	WBS/CES Description	Definitions	Source
1		IMDE Program Estimate WBS		
2	**1.0**	**Investment**	**All costs to the government to implement, fully, at all required operational sites, the system required to achieve and**	**DHS Standard IT WBS**
3	1.1	Program/Project Management	The program management element is defined as the business and administrative planning, organizing, directing,	DHS Standard IT WBS
4	1.1.1	Planning Phase Program/Project Management	This cost element includes the direct activities of persons performing program management functions in the planning	DHS Standard IT WBS
5	1.1.1.1	Government Personnel	This cost element includes the direct activities of government persons performing program management functions in the	DHS Standard IT WBS
5	1.1.1.2	Contractor Personnel	This cost element includes the direct activities of contractor personnel performing program management functions in the	DHS Standard IT WBS
5	1.1.1.3	Government TDY	This cost element includes the travel costs (e.g., transportation, per diem, etc.) of persons in the program management	DHS Standard IT WBS
5	1.1.1.4	Indirect Support	This cost element covers any indirect government personnel or other support related to program management. This	DHS Standard IT WBS
5	1.1.1.5	Non-labor	Roll-up	DHS Standard IT WBS
6	1.1.1.5.1	Contractor Travel	This cost element includes all non-labor costs, excluding TDY, associated with program management of the IT system	DHS Standard IT WBS
4	1.1.2	Acquisition Phase Program/Project Management	This cost element includes the direct activities of persons performing program management functions in the acquisition	DHS Standard IT WBS
5	1.1.2.1	Government Personnel	This cost element includes the direct activities of government persons performing program management functions in the	DHS Standard IT WBS
5	1.1.2.2	Contractor Personnel	This cost element includes the direct activities of contractor personnel performing program management functions in the	DHS Standard IT WBS
5	1.1.2.3	Government TDY	This cost element includes the travel costs (e.g., transportation, per diem, etc.) of persons in the program management	DHS Standard IT WBS
5	1.1.2.4	Indirect Support	This cost element covers any indirect government personnel or other support related to program management. This	DHS Standard IT WBS
5	1.1.2.5	Non-labor	Roll-up	DHS Standard IT WBS
6	1.1.2.5.1	Contractor Travel	This cost element includes all non-labor costs, excluding TDY, associated with program management of the IT system	DHS Standard IT WBS
4	1.1.3	Data Governance Activities	The process of determining the key performance characteristics, metric models, and trade spaces for mission performance	IMDE Analysis IPT
5	1.1.3.1	Planning Phase	Roll-up	
6	1.1.3.1.1	Initial Performance Reference Model	A performance reference model (PRM) is one of several reference models used in describing Federal Enterprise	IMDE Analysis IPT
7	1.1.3.1.1.1	Government Personnel	This cost element includes the direct activities of government persons performing program management functions in the	DHS Standard IT WBS
7	1.1.3.1.1.2	Contractor Personnel	This cost element includes the direct activities of contractor personnel performing program management functions in the	DHS Standard IT WBS
7	1.1.3.1.1.3	Government TDY	This cost element includes the travel costs (e.g., transportation, per diem, etc.) of persons in the program management	DHS Standard IT WBS
7	1.1.3.1.1.4	Indirect Support	This cost element covers any indirect government personnel or other support related to program management. This	DHS Standard IT WBS
7	1.1.3.1.1.5	Non-labor	This cost element covers any indirect government personnel or other support related to program management. This	DHS Standard IT WBS
8	1.1.3.1.1.5.1	Contractor Travel	This cost element includes the travel costs (e.g., transportation, per diem, etc.) of contractors as they conduct program	DHS Standard IT WBS
6	1.1.3.1.2	Threat Information Management	The processes of ensuring the BPR and SE teams have the appropriate level of threat information at the mission,	IMDE Analysis IPT
7	1.1.3.1.2.1	Initial Threat Assessment	The Initial Threat Environment Assessment provides capability developers and Program Managers (PM) the ability to assess	IMDE Analysis IPT
8	1.1.3.1.2.1.1	Government Personnel	This cost element includes the direct activities of government persons performing program management functions in the	DHS Standard IT WBS

ACEIT / Excel Demo

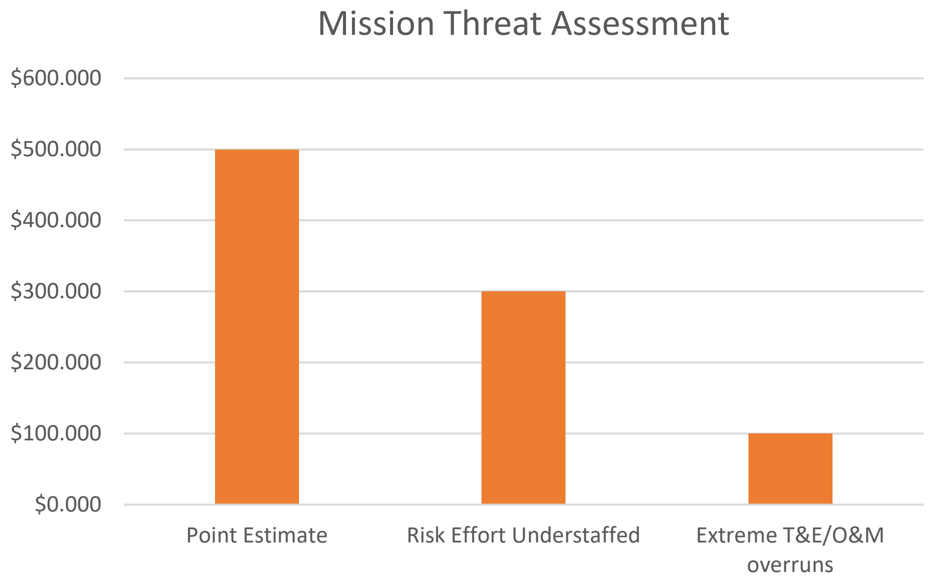
- 3 cases: best cast scenario, staffing risk (understaffed), and T&E/O&M overruns
- Comparisons if risk is not addressed early in the program or if additional support is needed during O&M afterwards

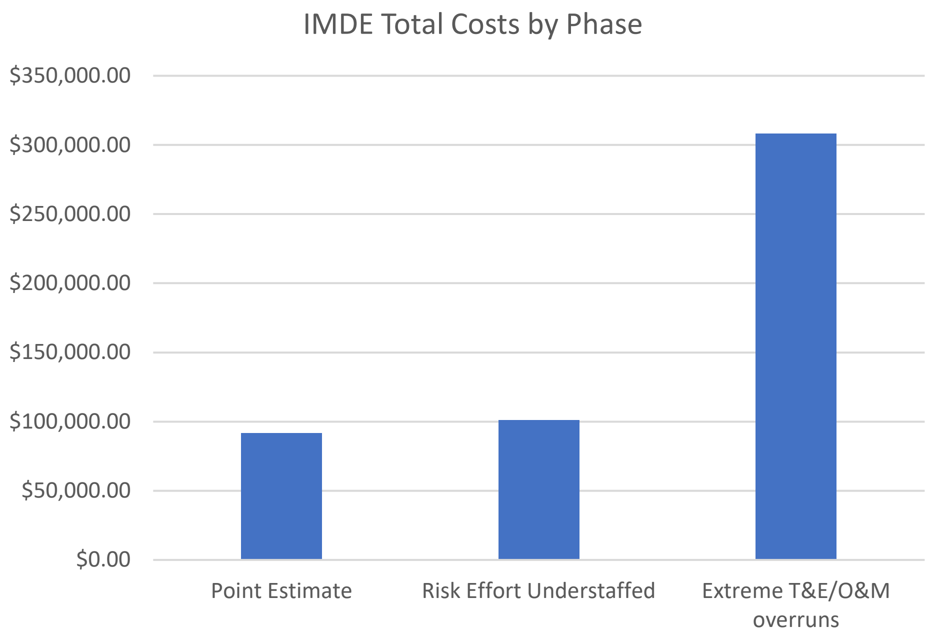


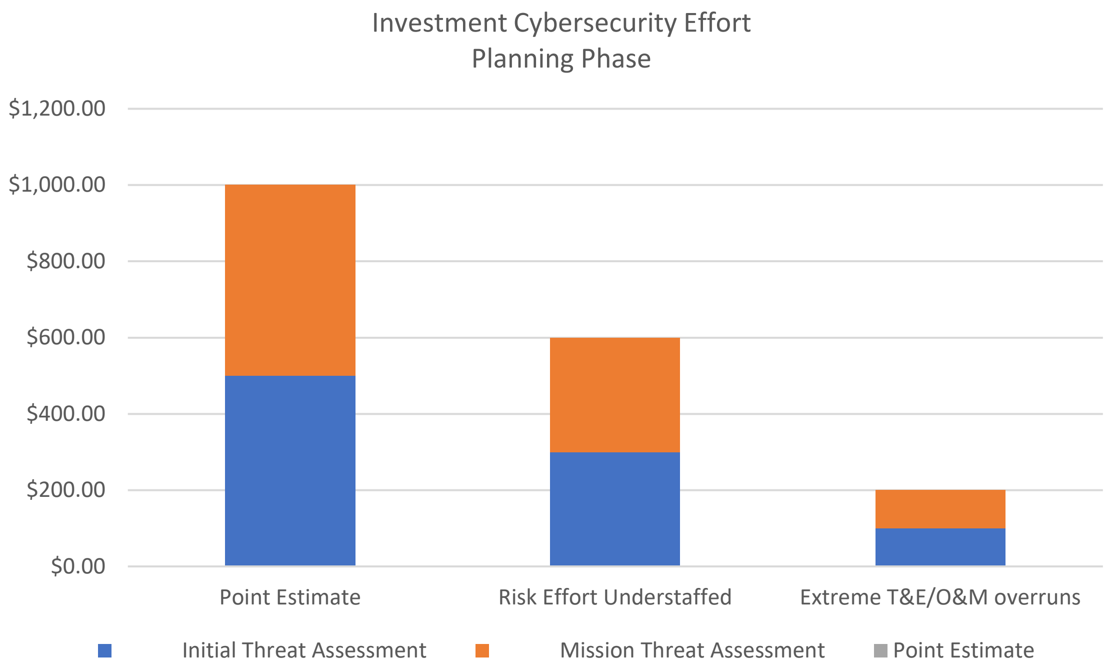
Row	WBS/CES Description	Comment	Unique ID	Point Estimate	Risk Effort Understaffed	Extreme T&E/ O&M overruns	Phasi
50	*Cases						
51	Case Switch (1=Best Case Scenario, 2=Risk Activity Understa		Switch	1.000	2.000	3.000	C
52							
53	*Case 2 (RA understaffed=>cost overrun in specific areas)						
54	Understaffed Factor		_Factor	1.000	0.300	0.100	C
55	*LOE Increase Factors due to Issues						
56	Planning BPR		_Factor	1.000	1.200	1.500	C
57	Acquisition BPR		_Factor	1.000	1.200	1.400	C
58	System Development	Architec	_Factor	1.000	1.500	2.000	C
59	T&E		_Factor	1.000	1.200	2.000	C
60	No Factor		_Factor	1.000	1.000	1.000	C
61	T&E post-FOC		_Factor	1.000	1.200	100.000	C
62							

ACEIT / Excel Demo

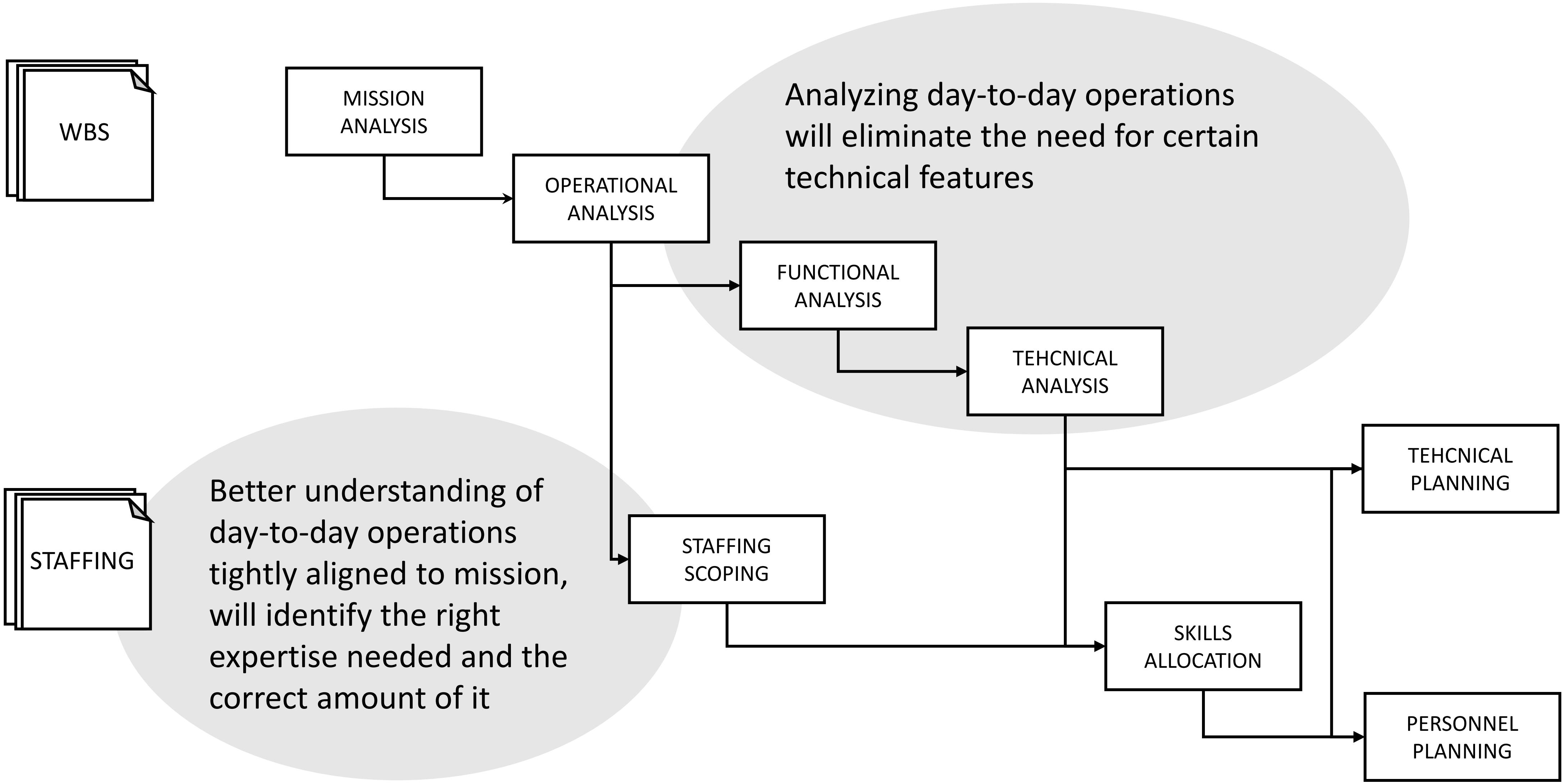
- Changing the factors: risk if understaffed and extreme T&E/O&M overruns results compared to the ideal for mission threat assessment and cybersecurity planning







IMDE Efficiencies



Analyzing day-to-day operations will eliminate the need for certain technical features

Better understanding of day-to-day operations tightly aligned to mission, will identify the right expertise needed and the correct amount of it

In Conclusion

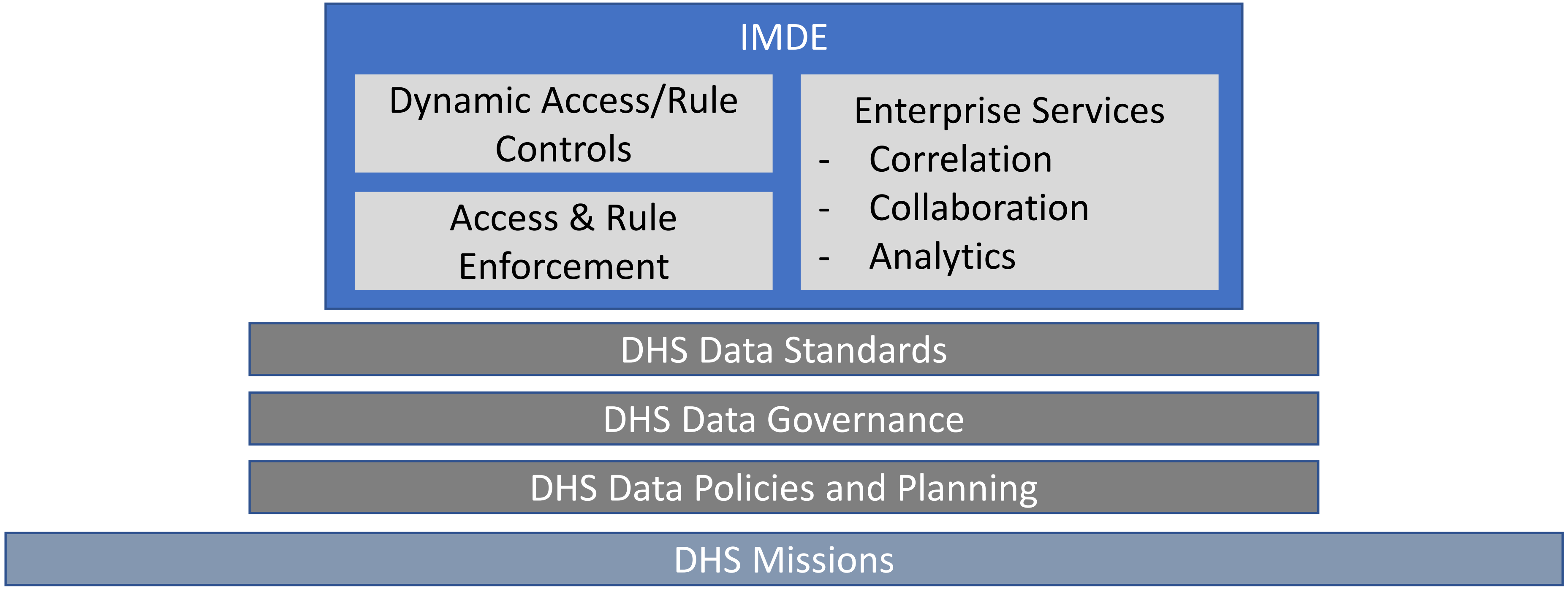
- IMDE is a pre-ADE-2A program
  - The proposed risk mitigation methodology will be tested and refined
- The methodology of identifying lower level WBS elements related to operational (not only technical risk) yields efficiencies and better mitigation outcomes

References

- Computer Security Division, Information Technology Laboratory. “About the RMF - NIST Risk Management Framework: CSRC.” *CSRC*, https://csrc.nist.gov/projects/risk-management/about-rmf.
- Computer Security Division, Information Technology Laboratory. “NIST Cybersecurity Framework: A Quick Start Guide - Cybersecurity Framework: CSRC.” *CSRC*, https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide.
- Insua, David Rios, et al. “An Adversarial Risk Analysis Framework for Cybersecurity”. *Risk Analysis*, vol. 41, no. 1, 2021. DOI: 10.1111/risa.13331.
- Lee, In. “Cybersecurity: Risk management framework and investment cost analysis”. *Business Horizons*, vol. 64, pp. 659-671. https://doi.org/10.1016/j.bushor.2021.02.022
- Radziwill, Nicole and Benton, Morgan. Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management. https://arxiv.org/ftp/arxiv/papers/1707/1707.02653.pdf.
- Russo, Mark. “The Illusion of Cybersecurity Quantification.” LinkedIn, Controlled Technical Services LLC, 26 Aug. 2021, https://www.linkedin.com/pulse/illusion-cybersecurity-quantification-?trk=organization-update-content_share-article.
- Taherdoost, Hamed. “Understanding Cybersecurity Frameworks and InformationSecurity Standards—A Review and Comprehensive Overview”. *Electronics.* https://doi.org/10.3390/electronics11142181.
- Krutilla , Kerry, et al. “The Benefits and Costs of Cybersecurity Risk Reduction: ADynamic Extension of the Gordon and Loeb Model”. *Risk Analysis*, vol. 41, no. 10, 2021. DOI: 10.1111/risa.13713.

Back-up

What is IMDE



IMDE

Dynamic Access/Rule Controls

Access & Rule Enforcement

Enterprise Services

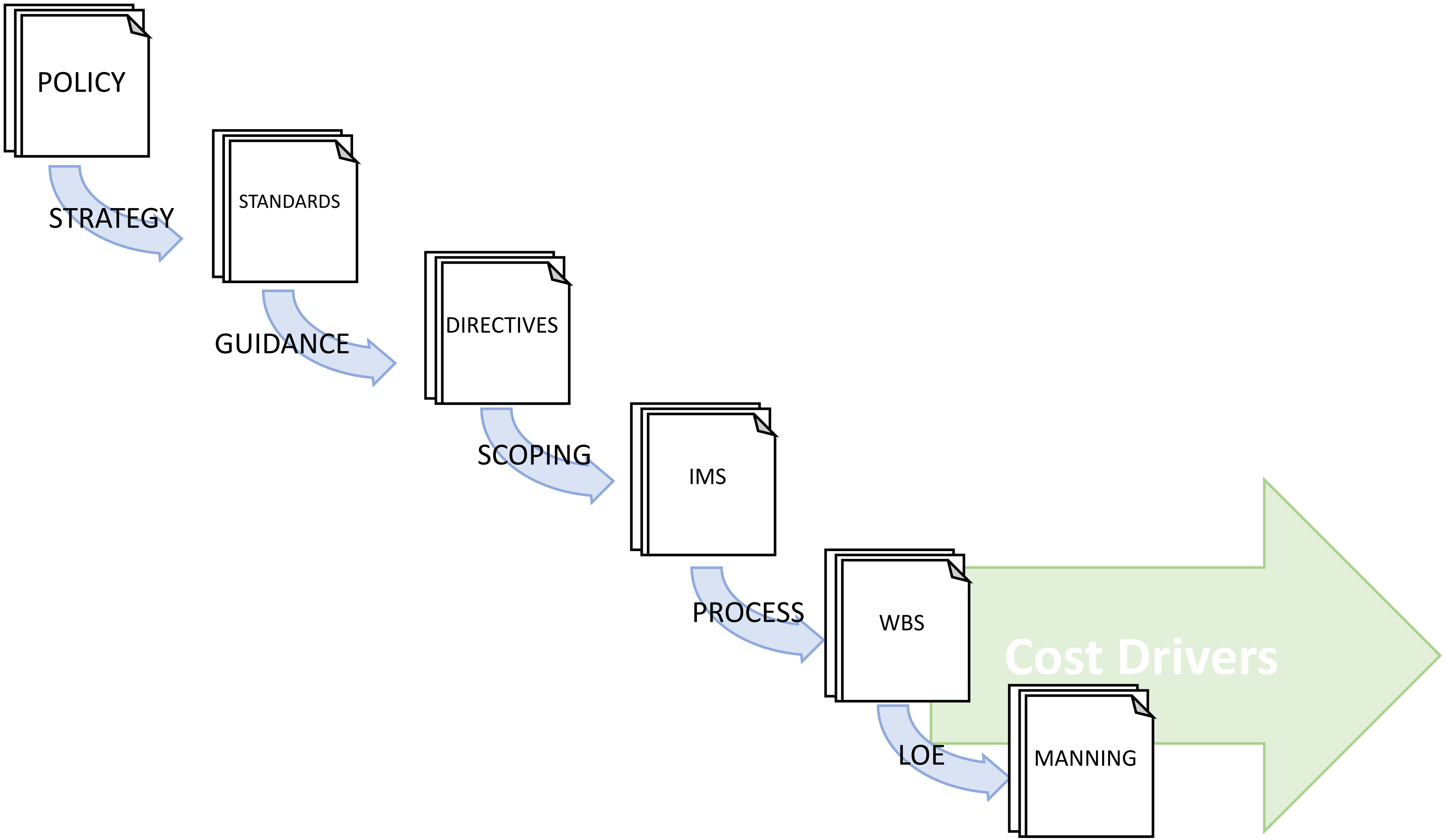
- Correlation
- Collaboration
- Analytics

DHS Data Standards

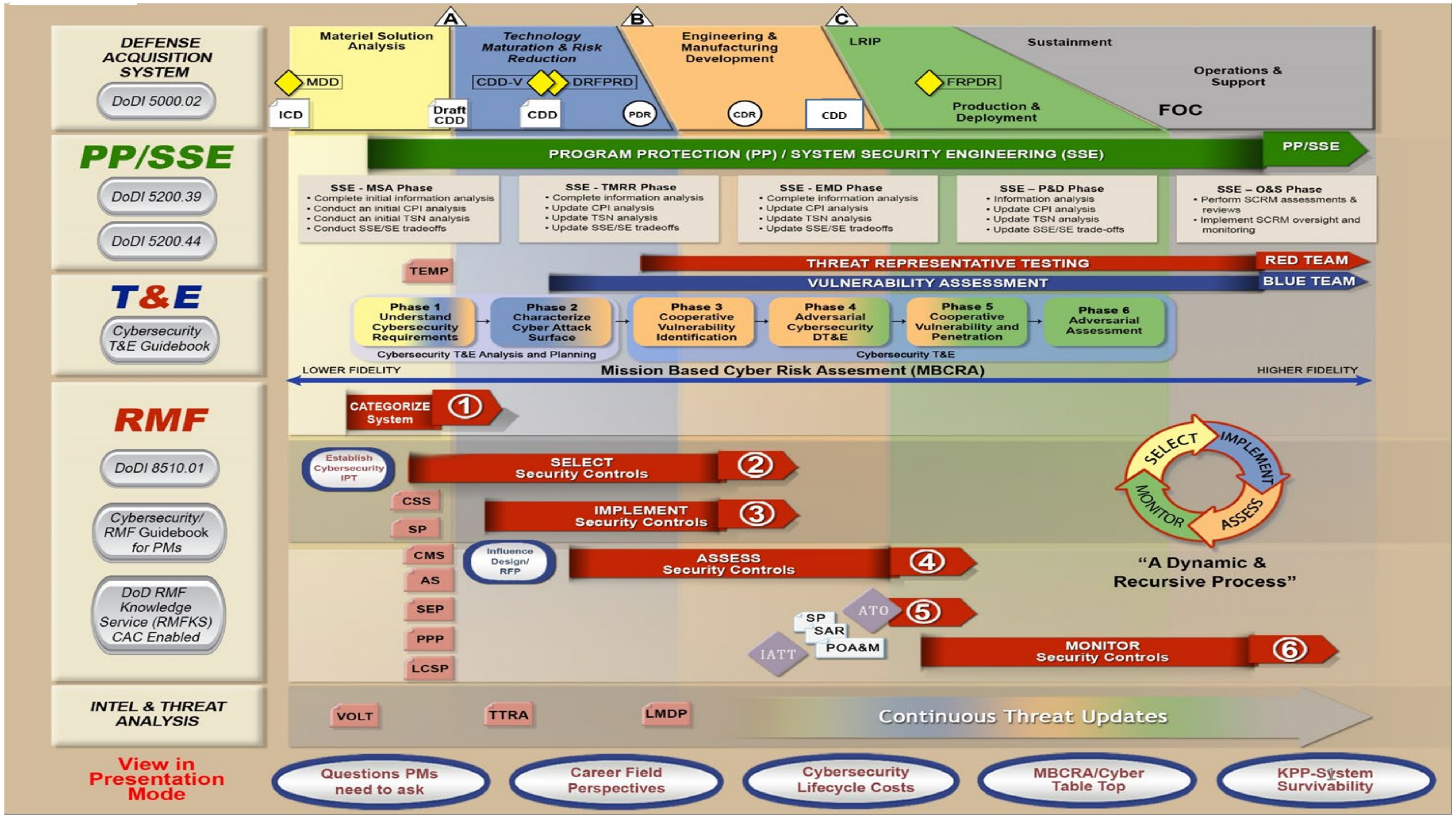
DHS Data Governance

DHS Data Policies and Planning

DHS Missions


POLICY
STRATEGY
STANDARDS
GUIDANCE
DIRECTIVES
SCOPING
IMS
PROCESS
WBS
LOE
MANNING
Cost Drivers

Cybersecurity in the Acquisition Lifecycle



DEFENSE ACQUISITION SYSTEM

DoDI 5000.02

A B C

Materiel Solution Analysis

Technology Maturation & Risk Reduction

Engineering & Manufacturing Development

LRIP

Sustainment

Operations & Support

MDD

CDD-V

DRFPRD

FRPDR

ICD

Draft CDD

CDD

PDR

CDR

CDD

Production & Deployment

FOC

PP/SSE

DoDI 5200.39

DoDI 5200.44

PROGRAM PROTECTION (PP) / SYSTEM SECURITY ENGINEERING (SSE)

PP/SSE

SSE - MSA Phase
- Complete initial information analysis
- Conduct an initial CPI analysis
- Conduct an initial TSN analysis
- Conduct SSE/SE tradeoffs

SSE - TMRR Phase
- Complete information analysis
- Update CPI analysis
- Update TSN analysis
- Update SSE/SE tradeoffs

SSE - EMD Phase
- Complete information analysis
- Update CPI analysis
- Update TSN analysis
- Update SSE/SE tradeoffs

SSE – P&D Phase
- Information analysis
- Update CPI analysis
- Update TSN analysis
- Update SSE/SE trade-offs

SSE – O&S Phase
- Perform SCRM assessments & reviews
- Implement SCRM oversight and monitoring

T&E

Cybersecurity T&E Guidebook

TEMP

THREAT REPRESENTATIVE TESTING

RED TEAM

VULNERABILITY ASSESSMENT

BLUE TEAM

Phase 1 Understand Cybersecurity Requirements → Phase 2 Characterize Cyber Attack Surface → Phase 3 Cooperative Vulnerability Identification → Phase 4 Adversarial Cybersecurity DT&E → Phase 5 Cooperative Vulnerability and Penetration → Phase 6 Adversarial Assessment

Cybersecurity T&E Analysis and Planning

Cybersecurity T&E

LOWER FIDELITY

Mission Based Cyber Risk Assesment (MBCRA)

HIGHER FIDELITY

RMF

DoDI 8510.01

Cybersecurity/ RMF Guidebook for PMs

DoD RMF Knowledge Service (RMFKS) CAC Enabled

CATEGORIZE System 1

Establish Cybersecurity IPT

SELECT Security Controls 2

CSS

SP

IMPLEMENT Security Controls 3

CMS

AS

SEP

PPP

LCSP

Influence Design/ RFP

ASSESS Security Controls 4

ATO 5

SP

SAR

POA&M

IATT

MONITOR Security Controls 6

SELECT

IMPLEMENT

ASSESS

MONITOR

"A Dynamic & Recursive Process"

INTEL & THREAT ANALYSIS

VOLT

TTRA

LMDP

Continuous Threat Updates

View in Presentation Mode

Questions PMs need to ask

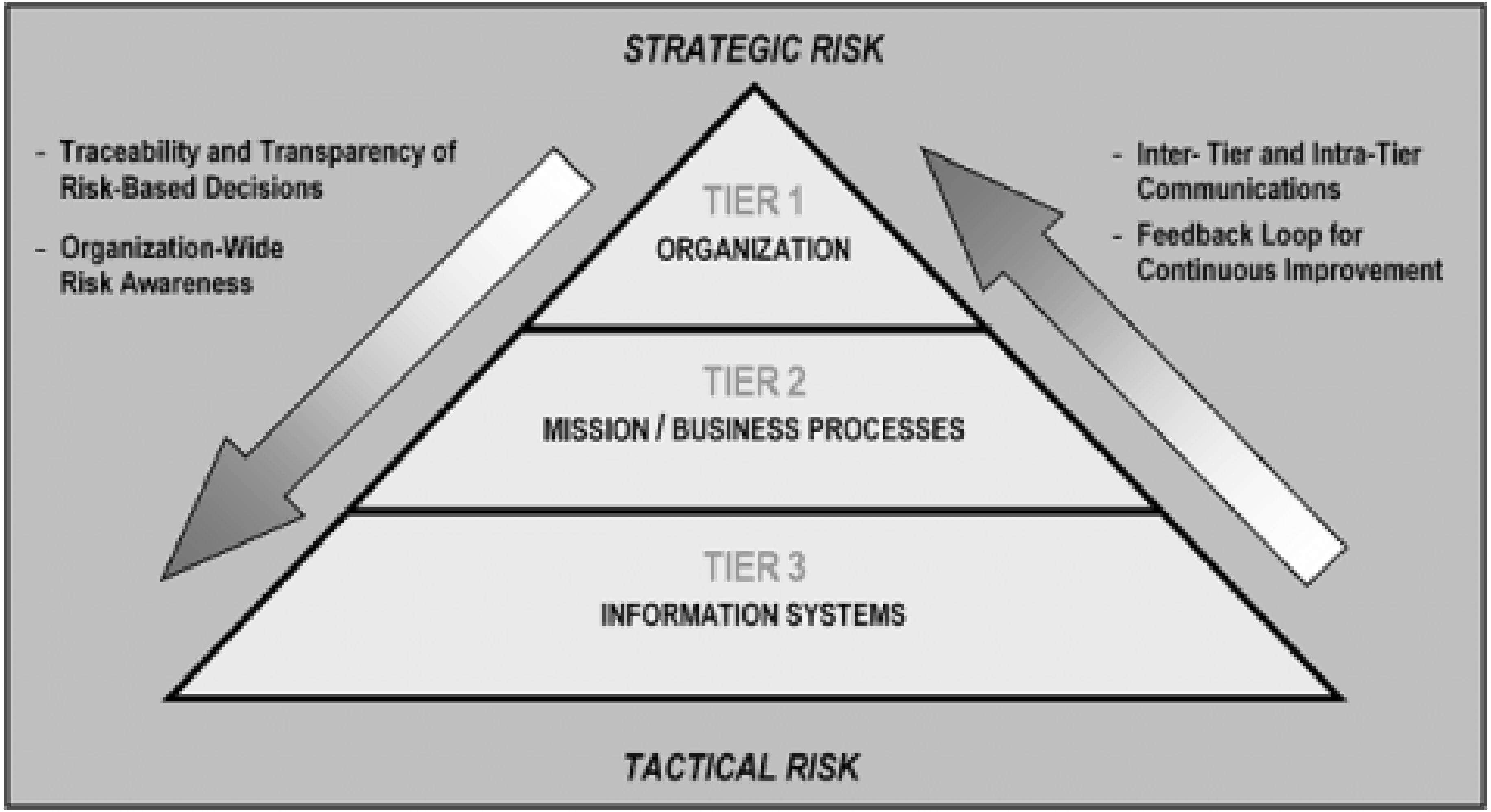
Career Field Perspectives

Cybersecurity Lifecycle Costs

MBCRA/Cyber Table Top

KPP-System Survivability

NIST 800-37 Risk Management Framework


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
TIER 1
ORGANIZATION
- Inter- Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK